

UNCLASSIFIED



# **NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY**



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

## **NDSLIC DISCLAIMER**

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

## **QUICK LINKS**

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including  
Schools and Universities\)](#)

[International](#)

[Information Technology and  
Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials  
Sector](#)

[National Monuments and Icons](#)

[Commercial Facilities](#)

[Postal and Shipping](#)

[Communications Sector](#)

[Public Health](#)

[Critical Manufacturing](#)

[Transportation](#)

[Defense Industrial Base Sector](#)

[Water and Dams](#)

[Emergency Services](#)

[North Dakota Homeland Security  
Contacts](#)

UNCLASSIFIED

## UNCLASSIFIED

### **NORTH DAKOTA**

Nothing Significant to Report

### **REGIONAL**

**(Minnesota) 8 injured in bull escape at Dakota County Fairgrounds.** Eight people were hurt August 7 at the Bulls and Barrels rodeo event at the Dakota County Fairgrounds after a bull escaped from a penned area. Source: <http://www.myfoxtwincities.com/story/23078244/injuries-reported-at-bulls-and-barrels-event-at-dakota-county-fairgrounds>

**(Montana) Man in custody after 75-mile chase in stolen ambulance.** An American Medical Response ambulance was stolen from a Billings restaurant parking lot August 3 and after leading police on a 75-mile chase, the driver crashed and was arrested near Big Horn County. Source: [http://mtstandard.com/news/local/state-and-regional/man-in-custody-after--mile-chase-in-stolen-ambulance/article\\_1f44425e-fd92-11e2-8654-001a4bcf887a.html](http://mtstandard.com/news/local/state-and-regional/man-in-custody-after--mile-chase-in-stolen-ambulance/article_1f44425e-fd92-11e2-8654-001a4bcf887a.html)

**(Montana) Crop damages estimated at millions of dollars in Gallatin County after storm.** A severe storm August 1 was believed to have caused millions of dollars of damage to Gallatin County crops. Source: <http://www.ktvq.com/news/crop-damages-estimated-at-millions-of-dollars-in-gallatin-county-after-storm/#>

**(South Dakota) Overnight fire at Watertown senior living complex.** Two residents were treated for minor injuries after the Sunchase Apartment Complex senior living facility in Watertown, South Dakota, was destroyed in a fire August 6. Officials are investigating the cause. Source: <http://www.keloland.com/newsdetail.cfm/overnight-fire-at-watertown-senior-living-complex/?id=151625>

### **NATIONAL**

**NSA: We read .00004% of Web traffic.** On the same day that President Barack Obama spoke to the press about possible surveillance reforms—and released a related white paper on the subject—the National Security Agency came out with its own rare, publicly-released, seven-page document (PDF), essentially justifying its own practices. Source: [http://www.cnn.com/2013/08/12/tech/web/nsa-privacy-email/index.html?hpt=us\\_c2](http://www.cnn.com/2013/08/12/tech/web/nsa-privacy-email/index.html?hpt=us_c2)

### **INTERNATIONAL**

**Some embassies to remain closed through Saturday.** The U.S. Department of State announced that several U.S. diplomatic posts worldwide will remain closed through August 10, while several others reopened August 5, after a terrorist threat was received. Source: <http://news.msn.com/us/some-embassies-to-remain-closed-through-saturday>

## UNCLASSIFIED

## **BANKING AND FINANCE INDUSTRY**

**Citizens Bank hit by DDOS attack, customers warned of intermittent interruption.** Citizens Bank warned customers August 8 that the bank's Web site was under distributed denial of service (DDoS) attack, which could cause service interruptions in online and mobile banking services. Source: <http://news.softpedia.com/news/Citizens-Bank-Hit-by-DDOS-Attack-Customers-Warned-of-Intermittent-Interruption-374242.shtml>

**U.S. accuses Bank of America of mortgage-backed securities fraud.** The U.S. Securities and Exchange Commission and U.S. Department of Justice filed two lawsuits against Bank of America for allegedly making misleading statements and failing to disclose important information about the mortgages behind a sale of \$850 million of residential mortgage-backed securities to investors in 2008. Source: <http://www.reuters.com/article/2013/08/06/us-bofa-justice-idUSBRE9750ZU20130806>

**Revealed: Cyberthug tool that BREAKS HSBC's anti-Trojan tech.** Group-IB spotted an exploit that bypasses part of Trusteer's Rapport anti-trojan system on underweb forums. Trusteer stated that the vulnerability only affects one layer of security and that a patch is being distributed to users. Source: [http://www.theregister.co.uk/2013/08/06/trusteer\\_pushes\\_updates\\_after\\_cybercreek\\_brew\\_up\\_browser\\_lockdown\\_exploit/](http://www.theregister.co.uk/2013/08/06/trusteer_pushes_updates_after_cybercreek_brew_up_browser_lockdown_exploit/)

**IPv6 is latest tool for stealing credit card numbers and passwords.** Security firm Neohapsis warned that the lack of implementation of the IPv6 protocol could allow attacks to monitor networks or redirect users to malicious pages by setting up a false IPv6 version of an IPv4 connection. Modern operating systems will then select the IPv6 connection due to their inbuilt preference for the protocol. Source: <http://www.v3.co.uk/v3-uk/news/2286734/ipv6-is-latest-tool-for-stealing-credit-card-numbers-and-passwords>

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**(Louisiana) Louisiana governor declares state of emergency due to train derailment, hazardous leaks.** The governor of Louisiana declared a state of emergency August 5 after a train derailed and leaked hazardous materials in Lawtell August 4. More than 20 cars went off the tracks near the intersection of U.S. Route 190 and Frank Road which prompted authorities to close U.S. Route 190 for at least 2 days and evacuate over 100 homes. Source: <http://www.wafb.com/story/23042516/developing-news-hazmat-crews-on-scene-of-lawtell-train-derailment>

## **COMMERCIAL FACILITIES**

**Walmart agrees to improve safety conditions at more than 2,800 stores.** Walmart agreed to improve worker training programs for operating hazardous equipment and use of cleaning chemicals in a settlement agreement with the U.S. Department of Labor announced August 7.

## UNCLASSIFIED

The agreement covers changes in 28 States or 2,857 Walmart stores that follow Occupational Safety and Health Administration standards as well as a \$190,000 fine to fix the hazards discovered during an inspection of a Rochester, New York store. Source:

[http://www.huffingtonpost.com/2013/08/07/walmart-safety-conditions\\_n\\_3719947.html](http://www.huffingtonpost.com/2013/08/07/walmart-safety-conditions_n_3719947.html)

### **COMMUNICATIONS SECTOR**

Nothing Significant to Report

### **CRITICAL MANUFACTURING**

**Toyota recalling 342,000 Tacoma pickups for seat belt problem.** Toyota announced a recall of 342,000 model year 2004-2011 Tacoma Access Cab vehicles due to the possibility of a screw to come loose which could cause seat belts to malfunction. Source:

<http://www.chicagotribune.com/classified/automotive/sns-rt-us-autos-toyota-recall-20130807,0,5385486.story>

**Defcon researchers reveal tricks behind their car hack.** Two security researchers delivered a presentation at the DEF CON 21 conference where they demonstrated how they were able to take control of several car systems and perform actions such as steering, acceleration, displaying incorrect speedometer readings, and others. Source:

<http://www.pcworld.com/article/2045895/researchers-reveal-methods-behind-car-hack-at-defcon.html>

### **DEFENSE/ INDUSTRY BASE SECTOR**

Nothing Significant to Report

### **EMERGENCY SERVICES**

**16 wildfires blamed on exploding shooting targets.** The use of exploding shooting targets, often made up of canisters containing two chemicals that blend and explode when struck by a bullet, were banned in 5 States by the U.S. Forest Service August 5 after authorities blamed the devices for sparking 16 wildfires since 2012. Source: <http://news.msn.com/us/16-wildfires-blamed-on-exploding-shooting-targets>

**Criminals hosting child pornography on 227 business websites.** Researchers at the Internet Watch Foundation found that 227 small and medium-sized businesses' Web sites were hijacked to store child pornography, possibly the first step in a ransomware or blackmail campaign.

Source: <http://www.v3.co.uk/v3-uk/news/2287093/criminals-hosting-child-pornography-on-227-business-websites>

UNCLASSIFIED

## **ENERGY**

**Workers begin drilling relief well to secure blow-out gas well in Gulf of Mexico.** Federal regulators announced drilling on a relief well to permanently seal the Walter Oil & Gas Corp. well that blew out in the Gulf of Mexico July 23 started August 4 and is expected to take about 35 days to complete. The cause of the blowout remains under investigation. Source: <http://www.dailyjournal.net/view/story/89109ec5cedf4b179ead24acdf6b7307/LA--Gas-Well-Leak>

## **FOOD AND AGRICULTURE**

**Cyclospora outbreak linked to Taylor Farms Salad, some served at Olive Garden and Red Lobster.** According to the U.S. Food and Drug Administration, the outbreak of Cyclospora in Iowa and Nebraska that caused hundreds of confirmed illnesses was linked to Mexican-grown Taylor Farms salad mix. Some of the contaminated salad mix was served at Olive Garden and Red Lobster restaurants and investigators believe the product expired and is no longer on the market. Source: <http://www.foodsafetynews.com/2013/08/cyclospora-outbreak-linked-to-taylor-farms-salad-some-served-at-olive-garden-and-red-lobster/>

## **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

**(Virginia) Network outage cripples Chesapeake City Hall.** Communication services including email, telephone services, and online services were down for several hours August 7 at the Chesapeake City Hall in Virginia due to an apparent failure in the computer network. Source: <http://hamptonroads.com/2013/08/network-outage-cripples-chesapeake-city-hall>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**Malicious snoopware targeting India found at tiny Midwest ISP.** ThreatConnect researchers traced a malware-based cyberespionage campaign targeting India to a small internet service provider (ISP) in Kansas City, Missouri. The researchers found booby-trapped .PDF files and Flash video files used in the campaign, as well as a .ZIP file of malware on the ISP's systems. Source: [http://www.theregister.co.uk/2013/08/07/india\\_cyberespionage/](http://www.theregister.co.uk/2013/08/07/india_cyberespionage/)

**Expect more Android security issues in 2013.** Trend Micro released their second quarter 2013 Security Roundup Report which found that the number of malicious and high-risk Android apps has grown rapidly from the previous quarter, to 718,000 from 509,000. Malware targeting online banking also grew, increasing 29 percent from the first quarter. Source: [https://www.net-security.org/malware\\_news.php?id=2555](https://www.net-security.org/malware_news.php?id=2555)

**Windows Phones BLAB passwords to hackers, thanks to weak crypto.** Microsoft warned users to take precautions after it was found that the encryption Windows Phones use to transmit domain credentials is cryptographically weak, allowing rogue hotspots to intercept and decrypt

## UNCLASSIFIED

the information. Microsoft advised IT departments to distribute a special root certificate that allows the phones to confirm that they are connecting to a genuine access point before transmission. Source:

[http://www.theregister.co.uk/2013/08/06/microsoft\\_win\\_phone\\_wifi\\_vuln/](http://www.theregister.co.uk/2013/08/06/microsoft_win_phone_wifi_vuln/)

**Phishing attacks show sudden drop as criminals use servers for DDoS.** The Anti-Phishing Working Group released their first quarter 2013 report, which found that detected phishing Web sites fell 20 percent in the quarter as cybercriminals switched servers to malware distribution or distributed denial of service (DDoS) attacks. Source:

<http://news.techworld.com/security/3462159/phishing-attacks-show-sudden-drop-as-criminals-use-servers-for-ddos/>

**Android one-click Google authentication method puts users, businesses at risk.** A Tripwire researcher at the DEF CON 21 conference detailed a way in which the weblogin feature on Google sites can be used to give attackers access to Google accounts. The researcher published a proof-of-concept app that can steal weblogin tokens and send them to the attacker for use. Source:

[https://www.computerworld.com/s/article/9241355/Android\\_one\\_click\\_Google\\_authentication\\_method\\_puts\\_users\\_businesses\\_at\\_risk](https://www.computerworld.com/s/article/9241355/Android_one_click_Google_authentication_method_puts_users_businesses_at_risk)

**Experts say 10 companies are responsible for 60% of Russian mobile malware.** Security firm Lookout released a study of Russian mobile malware and found that 10 organizations were responsible for creating 60% of mobile malware originating in Russia, among other findings. Source:

<http://news.softpedia.com/news/Experts-Say-10-Companies-Are-Responsible-for-60-of-Russian-Mobile-Malware-373107.shtml>

**Feds are suspects in new malware that attacks Tor anonymity.** A piece of malware that exploits a vulnerability in Firefox 17 and redirects connections over The Onion Router (TOR) network so users' true IP addresses can be discerned was found on several Web sites hosted by Freedom Hosting. Source: <http://www.wired.com/threatlevel/2013/08/freedom-hosting/>

**BREACH compression attack steals HTTPS secrets in under 30 seconds.** Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH) an attack that enables the reading of encrypted messages via plaintext injection into an HTTPS request, prompted an advisory after it was demonstrated at the Black Hat 2013 conference. Source:

<https://threatpost.com/breach-compression-attack-steals-https-secrets-in-under-30-seconds/101579>

## **NATIONAL MONUMENTS AND ICONS**

**(California) Aspen fire reported 80% contained.** Firefighters reached 80 percent containment August 7 of the 21,931-acre Aspen Fire burning north of Huntington Lake. Source:

<http://www.fresnobee.com/2013/08/07/3429755/aspen-fire-reported-80-contained.html>

## UNCLASSIFIED

## **POSTAL AND SHIPPING**

Nothing Significant to Report

## **PUBLIC HEALTH**

**Parasites infest more than 500 people; count up in 7 states.** The U.S. Centers for Disease Control and Prevention reported 504 confirmed Cyclospora infections in 16 States in the central and eastern parts of the country. Authorities are still investigating the transmission source for the parasite. Source: <http://www.foodsafetynews.com/2013/08/parasites-now-infect-more-than-500-people-numbers-up-in-seven-states/>

## **TRANSPORTATION**

**(New Jersey) N.J. man fined \$32K for illegal GPS device that disrupted Newark airport system.** A man from Readington was fined nearly \$32,000 after the Federal Communications Commission concluded he interfered with Newark Liberty International Airport's satellite-based tracking system when he used an illegal GPS jamming device in his pickup truck to hide his whereabouts from his employer. Source: [http://www.nj.com/news/index.ssf/2013/08/man\\_fined\\_32000\\_for\\_blocking\\_newark\\_airport\\_tracking\\_system.html](http://www.nj.com/news/index.ssf/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html)

**Airlines, airports hit by reservation system outage.** Sabre, a travel technology company, suffered a major outage August 5 for over 2 hours, impacting 400 airlines and 100 airports nationwide. Several national and international flights experienced delays because of a problem with a computer system they use for services such as reservations, check-ins, and online booking. Source: <http://news.msn.com/us/airlines-airports-hit-by-reservation-system-outage>

## **WATER AND DAMS**

**Chinese hacking team caught taking over decoy water plant.** A Trend Micro researcher presented the results of a project which set up fake industrial control systems purporting to be connected to water plant systems, and found that the Comment Crew/APT1 Chinese hacking group had targeted and compromised one decoy system, among other project results. Source: <http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/>

## **HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center: 866-885-8295(IN ND**

## UNCLASSIFIED

ONLY); Email: [ndslic@nd.gov](mailto:ndslic@nd.gov); Fax: 701-328-8175 **State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.**

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security [kihagel@nd.gov](mailto:kihagel@nd.gov), 701-328-8168

UNCLASSIFIED